trowers & hamlins

Legal update ——— October 2018

Dispute Resolution and Litigation
Technology, data and fraud

The way in which organisations buy and sell products and services has changed dramatically over the last 30 years. Advancements in technology have led to innovation, which in turn has fuelled competition amongst almost all industries and sectors.

If an organisation does not embrace technology, it risks falling behind its competitors who are able to offer the same product or service at a lower cost, or with a better customer experience. Obvious examples include the commercial deployment of augmented reality experiences (for example, Ikea's app which allows customers to see, through their mobile phones, what furniture could look like in their own homes), developments in the quality and viability of artificial intelligence (think driverless or autonomous vehicles, or even the new Amazon Go convenience stores) and the connection of every day devices (such as refrigerators, toasters and even showers) to the internet (also known as the Internet of Things).

The common theme with these products is that they create and capture data, which then provides that organisation or business with a competitive edge in its respective market. However, developments in technology are a double edged sword; on the one hand technology allows organisations to offer their services to customers and clients on a much broader scale (and potentially to whom they previously would not have been able to access), whilst on the other technology also acts as an enabler and gateway to fraud by allowing cyber criminals to mask who and where they are (and allowing them to catch victims off guard by orchestrating what appear to be legitimate schemes or activities).

The value of data is significant to both the organisation that holds it and to cyber criminals or fraudsters who wish to obtain it for illicit means. In fact, some have debated whether or not data is the new oil (attributing it to a commodity, which can be bought or sold). The true value is not just in what is being held, but what that data can be used for. For an organisation, knowing which products a potential customer is interested in can help it to send targeted emails (using predictive analytics and algorithms) and marketing information with a view to converting more sales of a product or service. However, for the fraudster, that data can be used in a whole host of ways. Addresses, dates of birth and other personal information could be used to identify further email accounts (which could be targeted for future fraud), or they could be used to begin to create seemingly legitimate accounts for the purposes of carrying out an identity theft. In addition, the speed at which funds or electronic assets can now be transferred can be devastating; the initial damage can be done in a very short space of time, but the long term damage to the individuals and organisations impacted can take much longer to resolve. The damage is not always financial, and in our experience it is the perceived lack of trust and reputational impact which is harder (sometimes impossible) to completely fix.

For many, GDPR was the kick start to addressing an organisation's risk to data theft; the emphasis having been shifted from being reactive, to proactive. It is now more important than ever (particularly where personal data is collated) that organisations consider their response plans and are in a better position to prevent (or at least identify) when they have been the subject of cybercrime. Failing to do so may mean that the ICO is not appropriately notified (or worse that the ICO elect to impose a financial sanction for contravening the GDPR). A solid response would allow the engagement of specialist legal, IT, accountancy and PR teams (as may be necessary) to minimise the potential disruption following an incident. It would also ensure that staff are trained and that appropriate processes and controls (likely by way of cyber security products) are in place.

We work with organisations to ensure that innovation is not discouraged, and that new opportunities can be exploited. If you would like to discuss your cyber response plan, or if you are concerned you may have been the victim or subject of cybercrime, please get in touch with Trowers & Hamlins to discuss your options.

Published by
Trowers & Hamlins

Trowers & Hamlins LLP
3 Bunhill Row
London
EC1Y 8YZ

t +44 (0)20 7423 8000
f +44 (0)20 7423 8001

www.trowers.com

For more information please contact

Mark Kenkre
Partner
t +44 (0)121 214 8863
e mkenkre@trowers.com

Christopher Recker
Associate
t +44 (0)121 214 8842
e crecker@trowers.com